PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-069419

(43)Date of publication of application : 12.03.1996

---

(51)Int.Cl. G06F 12/14

G06F 9/06

G06K 7/00

G06K 17/00

G09C 1/00

---

(21)Application number : 06-230603 (71)Applicant : SHIMADZU CORP

(22)Date of filing : 30.08.1994 (72)Inventor : NONAKA TAKANORI

---

(54) RECORDING DEVICE AND RECORDING MEDIUM FOR DIGITAL DATA

(57)Abstract:

PURPOSE: To provide the recording device and recording medium for digital data which can effectively prevent the digital data from illegally being copied.

CONSTITUTION: A data-supply side device 10 encodes the digital data recorded in a data base 11 by using a key code (y) generated by a key code generation part 14 and the identification code (x) which is characteristics of the recording medium FD and sent from a device 20. A data-reception side device 20 records the encoded data on the recording medium FD. The encoded data read out of the recording medium FD are decoded by a data decoding part 25 by using the key code (y) supplied from the device 10 and the identification code (x) of the recording medium FD which is read out by an identification code read part 24. The identification code on the recording medium FD is recorded on the recording medium FD in an unwritable state.

LEGAL STATUS [Date of request for examination] 14.06.2000

[Date of sending the examiner's decision of rejection] 27.07.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] A data storage means to memorize digital data, and an identification code input means to input the identification code of the record-medium proper which is going to record desired digital data, A keycode generating means to generate the keycode of arbitration, and an encryption means to encipher the digital data read from said data storage means using said identification code and said keycode, An output means to output said enciphered digital data (encryption data) and said keycode, An encryption data input means to input said encryption data, and a keycode input means to input said keycode, An encryption data-logging means to record said inputted encryption data on a record medium, An encryption data reading means to read the encryption data recorded on said record medium, An identification code reading means to read the identification code of said record-medium proper in the record medium itself, The recording device of the digital data characterized by having a data decode means to decode the encryption data read in said record medium to

the original digital data using the identification code read in said record medium itself, and said inputted keycode.

[Claim 2] The record medium which is a record medium with which digital data is recorded using the recording apparatus of digital data according to claim 1, and is characterized by what the identification code of the record-medium proper rewrites to said record medium, and is recorded on impossible.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Industrial Application] This invention relates to the equipment which records digital data, such as a computer program, and music, an image, alphabetic data, on a record medium, and the record medium used for this equipment, and relates to the technique of preventing the illegal copy of digital data especially.

[0002]

[Description of the Prior Art] Conventionally, as a record medium of digital data, various things, such as a magnetic tape, a magneto-optic disk, a semiconductor memory circuit, a floppy disk, and Hurd Thijs, are known. Digital data, such as a computer program, are recorded on this kind of record medium, and are supplied, or, recently, are supplied through a communication line.

[0003] A user can copy a computer program to other floppy disks, hard disks, etc. using his own computer. Moreover, recently, the equipment which records music and image information in digital one, for example like a compact disk has come to be

announced.

[0004] Thus, if the equipment which can record various kinds of software in digital one is developed, a user does not have degradation of the engine performance and can copy the software received from the feeder to other record media as it is. Music, an image, etc. can be received with a communication line or the means of broadcast, and a feeder can supply software without record media, such as a compact disk. Thereby, while the supply cost of software falls, a merit called resource saving is expected.

[0005]

[Problem(s) to be Solved by the Invention] However, the equipment which records digital data induces the problem of the illegal copy of software. In the computer program, the illegal copy already serves as a social problem.

[0006] Development cost is unrecoverable if the software developed when seen from a software feeder's position circulates by the unapproved copy. It cannot but stop setting up the selling price of software highly as the result.

[0007] On the other hand, seen from the position of the user who does an illegal copy, "software has the awareness of the issues of large sum past **", "paying a high amount of money also like software excellent also in inferior software, if it purchases to normal since it cannot purchase after confirming the contents like books", etc., and it is in the vicious circle condition of running to a copy involuntarily.

[0008] Although there is also a motion which is going to control an illegal copy legally, since it cannot do actually, discovering an illegal copy one by one in fact has a question in effectiveness. By computer software, supply in the form where the copy protection function was attached as a cure against an illegal copy etc. is performed now. It is earnestly examined by recording apparatus, such as music, as a cure against an illegal copy that the recorded data attach the function in which tone quality

etc. deteriorates rather than original data. Moreover, attaching the function in which the count of a copy is restricted etc. is examined.

[0009] These functions in which a copy is forbidden like, and the function in which the quality of software deteriorates at the time of a copy are to kill helplessly the advantage which is the property of digital storage equipment "the original source is recordable without degradation." Moreover, the social effectiveness that a feeder can supply software without a record medium to a user is not expectable, either. Moreover, seen from the position of the user who is going to use software justly, these functions are very inconvenient.

[0010] This invention is made in view of such a situation, and aims at offering the record medium used for the recording device of the digital data which can prevent an illegal copy effectively, and this equipment.

[0011]

[Means for Solving the Problem] This invention takes the following configurations, in order to attain such a purpose. Namely, the recording device of digital data according to claim 1 A data storage means to memorize digital data, and an identification code input means to input the identification code of the record-medium proper which is going to record desired digital data, A keycode generating means to generate the keycode of arbitration, and an encryption means to encipher the digital data read from said data storage means using said identification code and said keycode, An output means to output said enciphered digital data (encryption data) and said keycode, An encryption data input means to input said encryption data, and a keycode input means to input said keycode, An encryption data-logging means to record said inputted encryption data on a record medium, An encryption data reading means to read the encryption data recorded on said record medium, An identification code reading means to read the identification code of said record-medium proper in the

record medium itself, It has a data decode means to decode the encryption data read in said record medium to the original digital data using the identification code read in said record medium itself, and said inputted keycode.

[0012] A record medium according to claim 2 is a record medium with which digital data is recorded using the recording apparatus of digital data according to claim 1, and to said record medium, the identification code of the record-medium proper rewrites it, and it is recorded on impossible.

[0013]

[Function] The operation of invention according to claim 1 is as follows. When a user is going to receive supply of desired digital data, the identification code of the record-medium proper which is going to record the digital data is inputted through an identification code input means. The digital data taken out from the data storage means is enciphered by the encryption means using said identification code and the keycode generated from the keycode generating means. The digital data (encryption data) and the keycode which were enciphered are outputted through an output means. This encryption data is incorporated through an encryption data input means, and is recorded on the record medium which has said identification code with an encryption data-logging means. When using the digital data, by the encryption data reading means, encryption data are read in a record medium and it is sent to a data decode means. And encryption data are decoded using the keycode inputted through the identification code and the keycode input means which were read in the record medium itself by the identification code reading means.

[0014] Since identification code of the 2nd record medium cannot be rewritten to the same identification code as the 1st record medium even if it copies encryption data to another record medium (the 2nd record medium) from the record medium (the 1st record medium) with which encryption data were recorded according to invention

according to claim 2, even if it uses the equipment of claim 1, the encryption data copied to the 2nd record medium cannot be decoded.

[0015]

[Example] Hereafter, one example of this invention is explained with reference to a drawing.

<1st example> drawing 1 is the block diagram having shown the outline configuration of the 1st example of the recording apparatus of the digital data concerning this invention.

[0016] This example equipment consists of data supply side equipment 10 and data reception side equipment 20, and between both equipments is connected by the communication line L. Data supply side equipment 10 is installed in the selling firm which sells software. On the other hand, data reception side equipment 20 is an installing-in user side using software thing, and by drawing 1 , although much data reception side equipments 20 are tied through a communication line L to data supply side [one] equipment 10, since it is easy, it usually shows only data reception side [one] equipment 20. In addition, the installation part of each equipments 10 and 20 is arbitrary, in addition to the above-mentioned example, data supply side equipment 10 is installed in a software manufacturer, it installs data reception side equipment 20 in a software dealer, respectively, and a user goes to a software dealer and may be made to receive supply of desired software. Hereafter, the detailed configuration of each equipments 10 and 20 is explained.

[0017] Data supply side equipment 10 consists of the keycode generating sections 14, communication interfaces (I/F) 15, etc. which generate the keycode of the arbitration for the data base manager 12 which manages the database 11 which stored the software of varieties used as the candidate for selling, and a database 11, the encryption processing section 13 which enciphers software (digital data) with a supply

demand, and encryption. Here, the communication interface 15 is equivalent to the identification code input means and output means in this invention.

[0018] Data reception side equipment 20 A data demand command, the identification code of a record medium FD, etc. The encryption data reading section 23 for reading encryption data in the encryption data-logging section 22 for recording the control unit 21 which consists of a keyboard for inputting etc., and the encryption data sent from data supply side equipment 10 on a record medium FD, and a record medium FD, It consists of the data decode section 25 for decoding the identification code reading section 24 for reading identification code in a record medium FD, and encryption data, a communication interface 26, etc. Here, the communication interface 26 is equivalent to the encryption data input means and keycode input means in this invention.

[0019] Although especially the record medium FD does not limit the class, a floppy disk, a magnetic tape, a magneto-optic disk, a semiconductor memory circuit, Hurd Thijs, etc. are used, for example. In this record medium FD, the identification code of that record-medium proper rewrites, and it is beforehand recorded on impossible. Although not limited, especially the record technique of identification code records identification code on the field (protection field) which a user cannot rewrite magnetically, for example, or rewrites a bar code on the jacket front face on which the disc-like MAG sheet of a floppy disk was contained, and records it on impossible. The manufacturer who manufactures the record medium is a shipment phase, and records the identification code of such a record-medium proper with gestalten, such as the consecutive number, for every record medium, for example.

[0020] Next, the actuation in the case of receiving supply of software using the example equipment mentioned above is explained with reference to the flow chart of drawing 2 . In addition, S shows processing with data supply side equipment 10

among the subscript of each step number of drawing 2 , and U shows processing with data reception side equipment 20, respectively.

[0021] First, a user inputs data requiring [to wish / of software], and the identification code of the record medium FD which is going to record the data using the control unit 21 of data reception side equipment 20 (1U). This input is sent to data supply side equipment 10 through a communication line L. In addition, you may make it the identification code of a record medium FD send what was read in the identification code reading section 24 to data supply side equipment 10.

[0022] With data supply side equipment 10, a data base manager 12 picks out the digital data of software with a demand from a database 11 based on the data demand from data reception side equipment 20, and sends to the encryption processing section 13 (2S).

[0023] The encryption processing section 13 is enciphered using the identification code to which said digital data has been sent from data reception side equipment 20, and the keycode generated in the keycode generating section 14 in equipment 10 (3S).

[0024] The example which encryption processing of digital data simplified is explained below. Now, the identification code of f (t) and a record medium FD is expressed with x, and y (x) and encryption data are expressed [the digital data by which encryption processing is carried out] with g (t) for a keycode. For example, keycode y (x) is set as the function shown by degree type **.

y(x) =x3+Ex2+Fx ..... E and F are arbitrary constants in ** top type **.

[0025] Moreover, let encryption data g (t) be the function h (fx, y) shown by degree type **.

g(t)=h(f,x,y)

= f(t)+A(x2+Bx+C)+Dy+G ..... A, B, C, D, and G are arbitrary constants in ** top type

**.

[0026] If each function is set up as mentioned above, encryption data g (t) will substitute the function y of a keycode for the above-mentioned ** type, and will become like degree type **.

g(t)=(f(t)+A)(x2 +Bx+C)

+ D(x3+Ex2+Fx) +G ..... ** [0027] Data g (t) enciphered as mentioned above and keycode y (x) are transmitted to data reception side equipment 20 through a communication line L (4S).

[0028] With data reception side equipment 20, while the encryption data-logging section 22 records the transmitted encryption data on a record medium FD as it is, a keycode is accumulated in the data decode section 25 (5S).

[0029] When using the data recorded on the record medium FD, the encryption data reading section 23 reads encryption data from a record medium FD, and sends to the data decode section 25 (6U).

[0030] Moreover, the identification code reading section 24 reads in the record-medium FD itself the identification code recorded on the record medium FD, and sends the identification code to the data decode section 25 (7U).

[0031] The data decode section 25 decodes the encryption data read in the record medium FD to the original digital data using the keycode sent from data supply side equipment 10, and the identification code read in the identification code reading section 24 (8U).

[0032] It is as follows if the example by which the above [this decode processing] was simplified explains. inverse function h' (gx, y) expressed with degree type ** for the data decode section 25 to decode encryption data -- **** -- it is.

f(t)=h '(g,x,y)

= {(g(t)-G-Dy) /(x2+Bx+C)}-A ..... Original digital data f (t) is decoded by assigning the

value of the keycode y sent to the inverse function of ** above-mentioned type ** from data supply side equipment 10, and the identification code x read in the identification code reading section 24. That is, original digital data f (t) is reproduced by degree type **.

f(t) = -- [-- {(g(t)-G-D(x3+Ex2+Fx)} /(x2+ Bx+C)]-A ..... ** [0033]) Digital data f (t) decoded as mentioned above is sent to the use circuit section which data reception side equipment 20 does not illustrate.

[0034] Next, it explains that an illegal copy can be effectively prevented with the example equipment mentioned above. Temporarily, encryption data are recorded on the predetermined record medium FD (henceforth the 1st record medium) by the above-mentioned processing, and suppose that that encryption data was copied to another record medium (henceforth the 2nd record medium) from this 1st record medium. When it is going to set and decrypt the 2nd record medium to the data reception side equipment 20 of an example, the identification code of the 2nd record medium read in the identification code reading section 24 becomes a different thing from the identification code of the 1st record medium. Therefore, even if it passes the identification code to the data decode section 25, the encryption data enciphered using the identification code of the 1st record medium cannot be decoded.

[0035] The example of the equipment for copying lawfully the <2nd example>, next the supplied digital data by the user side is explained with reference to drawing 3 . Drawing 3 is the outline block diagram of the data reception side equipment 20 to which the configuration for copying lawfully was added. Among drawing, since the component shown with the same sign as the sign shown in drawing 1 is the same component as the 1st above-mentioned example, explanation here is omitted. Moreover, since data supply side equipment 10 is the same as that of the 1st example, explanation here is omitted.

[0036] The data reception side equipment 20 shown in drawing 3 is equipped with the encryption data-logging section 28 for recording the encryption processing section 27 for newly enciphering the digital data decoded in the data decode section 25 as a configuration for copying the supplied digital data, and new encryption data on another record medium FD 2.

[0037] A user uses the control unit 21 of data reception side equipment 20 to copy data to another record medium FD 2 from the record medium FD 1 recorded first, and it is identification code x2 of the demand of a data copy to data supply side equipment 10, and a record medium FD 2. It sends. Based on this demand, data supply side equipment 10 sends the new keycode y2 (x2) to data reception side equipment 20. This keycode y2 It is given to the encryption processing section 27 of data reception side equipment 20. Moreover, a user uses a control unit 21 and is identification code x2 of the new record medium FD 2. It inputs. This identification code x2 It is given to the encryption processing section 27. The encryption processing section 27 is a keycode y2. Identification code x2 It uses and the digital data outputted from the data decode section 25 is enciphered again. New encryption data g2 It is recorded on a record medium FD 2 by the encryption data-logging section 29.

[0038] If the record medium FD 2 copied as mentioned above is changed into the original record medium FD 1 and it sets to data reception side equipment 20, the data decode section 25 will be a keycode y2. Identification code x2 of the record medium FD 2 read in the identification code reading section 24 It uses and is the encryption data g2 of a record medium FD 2. The copied digital data f can be used by decoding.

[0039] <3rd example> drawing 4 and drawing 5 are referred to. The block diagram in which drawing 4 showed the outline configuration of data supply side equipment, and drawing 5 are the block diagrams having shown the outline configuration of data reception side equipment.

[0040] It is installed in a software dealer etc. and the data supply side equipment shown in drawing 4 is equipped with the encryption data-logging section 22 which records the enciphered digital data g on a record medium FD. A user's hope of the purchase of a certain software specifies the software from control unit 21A. The digital data of the specified software is enciphered in the encryption processing section 13 using the identification code x of the record medium FD inputted from control unit 21A, and the keycode y generated from the keycode generating section 14. The enciphered digital data g is given to the encryption data-logging section 22 through an interface 17, and after being recorded on a record medium FD in this encryption data-logging section 22, it is handed to a user (sold). The printout of the keycode y for decoding encryption data is carried out by the printer 16, and it is handed to a user.

[0041] The user who purchased software decodes encryption data with the data reception side equipment shown in drawing 5 . That is, with data reception side equipment, while the identification code x of a record medium FD is read by the identification code reading section 24, Keycode y is inputted by the user through control unit 21B. The data decode section 25 decodes the encryption data g using the identification code x and Keycode y which were mentioned above, and outputs them to the use circuit section.

[0042]

[Effect of the Invention] According to this invention, the following effectiveness is done so so that clearly from the above explanation. Since the digital data enciphered using the keycode of arbitration and the identification code of a record-medium proper is recorded on a record medium with the discernment coat according to the recording device of digital data according to claim 1 Even if it copies the encryption data recorded on the record medium (the 1st record medium) to another record medium (the 2nd record medium), since the identification code of the 2nd record medium

differs from the identification code of the 1st record medium, the encryption data copied to the 2nd record medium cannot be decoded. Therefore, according to this equipment, the illegal copy of digital data can be prevented effectively.

[0043] Moreover, since according to the record medium according to claim 2 the identification code of the record-medium proper rewrites to a record medium and it is recorded on impossible, by rewriting the identification code of the 2nd record medium to the identification code of the 1st record medium in the above-mentioned example, it cannot say that encryption data are decoded but prevention of the illegal copy of digital data can be made into a positive thing.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram having shown the outline configuration of the 1st example equipment.

[Drawing 2] It is the operation flow chart of the 1st example equipment.

[Drawing 3] It is the block diagram having shown the outline configuration of the data reception side equipment of the 2nd example equipment.

[Drawing 4] It is the block diagram having shown the outline configuration of the data supply side equipment of the 3rd example equipment.

[Drawing 5] It is the block diagram having shown the outline configuration of the data reception side equipment of the 3rd example equipment.

[Description of Notations]

10 -- Data supply side equipment

11 -- Database

13 -- Encryption processing section

14 -- Keycode generating section

15 26 -- Communication interface

20 -- Data reception side equipment

21 -- Control unit

22 -- Encryption data-logging section

23 -- Encryption data reading section

24 -- Identification code reading section

25 -- Data decode section

FD -- Record medium

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平8－69419

(43)公開日　平成８年(1996)３月12日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　12/14	３２０　Ｆ			
	Ｂ			
9/06	５５０　Ｃ	7230－5B		
	Ｘ	7230－5B		
Ｇ０６Ｋ　7/00	Ｗ	7623－5B		

審査請求　未請求　請求項の数２　ＦＤ　（全　８　頁）　最終頁に続く

(21)出願番号　特願平6－230603

(22)出願日　平成６年(1994)８月30日

(71)出願人　000001993
株式会社島津製作所
京都府京都市中京区西ノ京桑原町１番地

(72)発明者　埜中　孝則
京都市中京区西ノ京桑原町１番地　株式会社島津製作所三条工場内

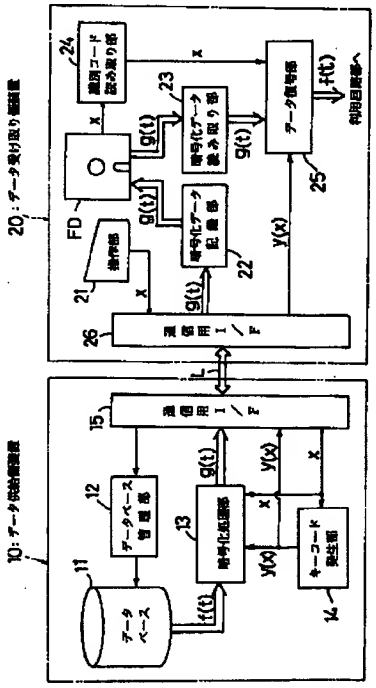
(74)代理人　弁理士　杉谷　勉

(54)【発明の名称】　デジタルデータの記録装置および記録媒体

(57)【要約】

【目的】　デジタルデータの違法コピーを有効に防止することができるデジタルデータの記録装置および記録媒体を提供する。

【構成】　データ供給側装置１０では、データベース１１に記録されたデジタルデータを、キーコード発生部１４で発生させたキーコードｙと、装置２０から送られてきた記録媒体ＦＤ固有の識別コードｘとを使って暗号化する。データ受け取り側装置２０では暗号化データを記録媒体ＦＤに記録する。記録媒体ＦＤから読み出された暗号化データは、装置１０から与えられたキーコードｙと、識別コード読み取り部２４で読み取られた記録媒体ＦＤの識別コードｘとを使ってデータ復号部２５で復号される。記録媒体ＦＤの識別コードは書き換え不能に記録媒体ＦＤに記録されている。



1

【特許請求の範囲】

【請求項１】　デジタルデータを記憶するデータ記憶手段と、所望のデジタルデータを記録しようとする記録媒体固有の識別コードを入力する識別コード入力手段と、任意のキーコードを発生するキーコード発生手段と、前記データ記憶手段から読み出されたデジタルデータを前記識別コードと前記キーコードとを使って暗号化する暗号化手段と、前記暗号化されたデジタルデータ（暗号化データ）および前記キーコードを出力する出力手段と、前記暗号化データを入力する暗号化データ入力手段と、前記キーコードを入力するキーコード入力手段と、前記入力された暗号化データを記録媒体に記録する暗号化データ記録手段と、前記記録媒体に記録された暗号化データを読み取る暗号化データ読み取り手段と、前記記録媒体固有の識別コードをその記録媒体自身から読み取る識別コード読み取り手段と、前記記録媒体から読み取られた暗号化データを、前記記録媒体自身から読み取られた識別コードと前記入力されたキーコードとを使って元のデジタルデータに復号するデータ復号手段とを備えたことを特徴とするデジタルデータの記録装置。

【請求項２】　請求項１に記載のデジタルデータの記録装置を使ってデジタルデータが記録される記録媒体であって、前記記録媒体には、その記録媒体固有の識別コードが書き換え不能に記録されていることを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明は、コンピュータプログラムや音楽・映像・文字データなどのデジタルデータを記録媒体へ記録する装置、およびこの装置に使用される記録媒体に係り、特に、デジタルデータの違法コピーを防止する技術に関する。

【０００２】

【従来の技術】従来、デジタルデータの記録媒体としては例えば、磁気テープ、光磁気ディスク、半導体メモリ回路、フロッピーディスク、ハードディスクなど種々のものが知られている。コンピュータプログラムなどのデジタルデータは、この種の記録媒体に記録されて供給されたり、あるいは最近では通信回線を介して供給されるようになっている。

【０００３】ユーザは、コンピュータプログラムを自分のコンピュータを使って他のフロッピーディスクやハードディスクなどにコピーすることができる。また、最近では、例えばコンパクトディスクのように音楽や映像情報をデジタルで記録する装置が発表されるようになってきた。

【０００４】このように、各種のソフトウェアをデジタルで記録できる装置が開発されると、ユーザは供給者から受け取ったソフトウェアを性能の劣化なく、そのまま他の記録媒体にコピーすることができる。音楽や映像など

2

も通信回線や放送といった手段で受け取ることができ、供給者はコンパクトディスクなどの記録媒体なしでソフトウェアを供給することができる。これにより、ソフトウェアの供給コストが下がるとともに、資源節約というメリットなどが期待される。

【０００５】

【発明が解決しようとする課題】しかしながら、デジタルデータを記録する装置は、ソフトウェアの違法コピーという問題を生む。コンピュータプログラムでは既に違法コピーが社会問題となっている。

【０００６】ソフトウェア供給者の立場から見ると、開発したソフトウェアが無断コピーによって流通してしまうと開発コストを回収できない。その結果としてソフトウェアの販売価格を高く設定せざるを得なくなる。

【０００７】一方、違法コピーをするユーザの立場からみると、『ソフトウェアが高額過ぎる』、『書籍のように内容を確かめてから購入することができないので、正規に購入すると劣悪なソフトウェアにも優秀なソフトウェアにも同様に高い金額を支払ってしまう』などの問題意識をもっており、思わずコピーに走ってしまうという悪循環状態になっている。

【０００８】違法コピーを法的に取り締まろうとする動きもあるが、実際には違法コピーをいちいち発見することは現実的にはできないので効果に疑問がある。コンピュータソフトでは、違法コピー対策としてコピープロテクト機能をつけた形での供給などが現在行われている。音楽などの記録装置では、違法コピー対策として、記録されたデータはオリジナルデータよりも音質などが劣化するような機能を付けることが真剣に検討されている。また、コピー回数を制限するような機能を付けることなども検討されている。

【０００９】これらのように、コピーを禁止するような機能やコピー時にソフトウェアの質が劣化するような機能は、デジタル記録装置の特性である『劣化なくオリジナルソースを記録できる』という長所をみすみす殺すことになっている。また、記録媒体なしに供給者がユーザにソフトウェアを供給することができるという社会的効果も期待できない。また正当にソフトウェアを利用しようとするユーザの立場からみると、これらの機能は不便そのものである。

【００１０】この発明は、このような事情に鑑みてなされたものであって、違法コピーを有効に防止することができるデジタルデータの記録装置、およびこの装置に用いられる記録媒体を提供することを目的としている。

【００１１】

【課題を解決するための手段】この発明は、このような目的を達成するために、次のような構成をとる。すなわち、請求項１に記載のデジタルデータの記録装置は、デジタルデータを記憶するデータ記憶手段と、所望のデジタルデータを記録しようとする記録媒体固有の識別コー

ドを入力する識別コード入力手段と、任意のキーコードを発生するキーコード発生手段と、前記データ記憶手段から読み出されたデジタルデータを前記識別コードと前記キーコードとを使って暗号化する暗号化手段と、前記暗号化されたデジタルデータ（暗号化データ）および前記キーコードを出力する出力手段と、前記暗号化データを入力する暗号化データ入力手段と、前記キーコードを入力するキーコード入力手段と、前記入力された暗号化データを記録媒体に記録する暗号化データ記録手段と、前記記録媒体に記録された暗号化データを読み取る暗号化データ読み取り手段と、前記記録媒体固有の識別コードをその記録媒体自身から読み取る識別コード読み取り手段と、前記記録媒体から読み取られた暗号化データを、前記記録媒体自身から読み取られた識別コードと前記入力されたキーコードとを使って元のデジタルデータに復号するデータ復号手段とを備えたものである。

【００１２】請求項２に記載の記録媒体は、請求項１に記載のデジタルデータの記録装置を使ってデジタルデータが記録される記録媒体であって、前記記録媒体には、その記録媒体固有の識別コードが書き換え不能に記録されている。

【００１３】

【作用】請求項１に記載の発明の作用は次のとおりである。ユーザが所望のデジタルデータの供給を受けようとする場合、そのデジタルデータを記録しようとする記録媒体固有の識別コードが識別コード入力手段を介して入力される。データ記憶手段から取り出されたデジタルデータは、前記識別コードとキーコード発生手段から発生されたキーコードとを使って、暗号化手段によって暗号化される。暗号化されたデジタルデータ（暗号化データ）とキーコードとが出力手段を介して出力される。この暗号化データは暗号化データ入力手段を介して取り込まれ、暗号化データ記録手段によって前記識別コードをもつ記録媒体に記録される。そのデジタルデータを利用する場合には、暗号化データ読み取り手段によって記録媒体から暗号化データが読み取られてデータ復号手段に送られる。そして、識別コード読み取り手段によってその記録媒体自身から読み取られた識別コードとキーコード入力手段を介して入力されたキーコードとを使って、暗号化データが復号される。

【００１４】請求項２に記載の発明によれば、暗号化データが記録された記録媒体（第１記録媒体）から別の記録媒体（第２記録媒体）へ暗号化データをコピーしたとしても、第２記録媒体の識別コードを第１記録媒体と同じ識別コードに書き換えることができないので、請求項１の装置を使っても第２記録媒体にコピーされた暗号化データを復号することはできない。

【００１５】

【実施例】以下、図面を参照してこの発明の一実施例を説明する。

＜第１実施例＞図１は、この発明に係るデジタルデータの記録装置の第１実施例の概略構成を示したブロック図である。

【００１６】この実施例装置は、データ供給側装置１０とデータ受け取り側装置２０とから構成され、両装置間が通信回線Ｌで接続されている。データ供給側装置１０は、ソフトウェアを販売する販売会社などに設置されるものである。一方、データ受け取り側装置２０は、ソフトウェアを利用するユーザ側に設置されるのもので、通常、一つのデータ供給側装置１０に対して多数のデータ受け取り側装置２０が通信回線Ｌを介して結ばれるが、図１では簡単のために一つのデータ受け取り側装置２０のみを示している。なお、各装置１０，２０の設置個所は任意であり、上記の例以外に、データ供給側装置１０をソフトウェア・メーカに、データ受け取り側装置２０をソフトウェア販売店にそれぞれ設置し、ユーザがソフトウェア販売店に出向いて所望のソフトウェアの供給を受けるようにしてもよい。以下、各装置１０，２０の詳細な構成を説明する。

【００１７】データ供給側装置１０は、販売対象となる多種類のソフトウェアを格納したデータベース１１、データベース１１を管理するデータベース管理部１２、供給要求のあったソフトウェア（デジタルデータ）を暗号化する暗号化処理部１３、暗号化のための任意のキーコードを発生するキーコード発生部１４、通信用インターフェース（Ｉ／Ｆ）１５などから構成されている。ここで、通信用インターフェース１５は本発明における識別コード入力手段および出力手段に相当している。

【００１８】データ受け取り側装置２０は、データ要求指令や記録媒体ＦＤの識別コードなどを入力するためのキーボードなどからなる操作部２１、データ供給側装置１０から送られてきた暗号化データを記録媒体ＦＤに記録するための暗号化データ記録部２２、記録媒体ＦＤから暗号化データを読み取るための暗号化データ読み取り部２３、記録媒体ＦＤから識別コードを読み取るための識別コード読み取り部２４、暗号化データを復号するためのデータ復号部２５、通信用インターフェース２６などから構成されている。ここで、通信用インターフェース２６は本発明における暗号化データ入力手段およびキーコード入力手段に相当している。

【００１９】記録媒体ＦＤは、特にその種類を限定しないが、例えばフロッピーディスク、磁気テープ、光磁気ディスク、半導体メモリ回路、ハードディスクなどが用いられる。この記録媒体ＦＤには、その記録媒体固有の識別コードが書き換え不能に予め記録されている。識別コードの記録手法は特に限定しないが、例えば、ユーザが書き換えできない領域（プロテクト領域）に識別コードを磁気的に記録しておいたり、あるいはフロッピーディスクの円盤状磁気シートが収納されたジャケット表面にバーコードを書き換え不能に記録しておく。このような

5

記録媒体固有の識別コードは例えば、その記録媒体を製造するメーカが出荷段階で、各記録媒体ごとに例えば連続番号などの形態で記録しておく。

【００２０】次に上述した実施例装置を使ってソフトウェアの供給を受ける場合の動作を図２のフローチャートを参照して説明する。なお、図２の各ステップ番号の添字中、Ｓはデータ供給側装置１０での処理、Ｕはデータ受け取り側装置２０での処理をそれぞれ示している。

【００２１】まず、ユーザが、データ受け取り側装置２０の操作部２１を使って、希望するソフトウェアのデータ要求と、そのデータを記録しようとする記録媒体ＦＤの識別コードとを入力する（１Ｕ）。この入力情報は通信回線Ｌを介してデータ供給側装置１０に送られる。なお、記録媒体ＦＤの識別コードは、識別コード読み取り部２４で読み取ったものをデータ供給側装置１０に送るようにしてもよい。

＊

$$y(x)=x^3+Ex^2+Fx \quad \cdots\cdots①$$

上式①でＥ，Ｆは任意定数である。

【００２５】また、暗号化データｇ（ｔ）を次式②で示※

$$g(t)=h(f,x,y)=(f(t)+A)(x^2+Bx+C)+Dy+G \quad \cdots\cdots②$$

上式②で、Ａ，Ｂ，Ｃ，Ｄ，Ｇは任意定数である。

【００２６】上記のように各関数を設定すると、暗号化★

$$g(t)=(f(t)+A)(x^2+Bx+C)+D(x^3+Ex^2+Fx)+G \quad \cdots\cdots③$$

【００２７】上記のようにして暗号化されたデータｇ（ｔ）と、キーコードｙ（ｘ）とを通信回線Ｌを介してデータ受け取り側装置２０に伝送する（４Ｓ）。

【００２８】データ受け取り側装置２０では、伝送されてきた暗号化データを暗号化データ記録部２２が記録媒体ＦＤにそのまま記録するとともに、キーコードをデータ復号部２５に蓄積する（５Ｓ）。

【００２９】記録媒体ＦＤに記録されたデータを利用する場合は、暗号化データ読み取り部２３が記録媒体ＦＤから暗号化データを読み出してデータ復号部２５に送る（６Ｕ）。

【００３０】また、識別コード読み取り部２４が記録媒☆

$$f(t)=h'(g,x,y)=\{(g(t)-G-Dy)/(x^2+Bx+C)\}-A \quad \cdots\cdots④$$

上記式④の逆関数にデータ供給側装置１０から送られてきたキーコードｙと、識別コード読み取り部２４で読み取られた識別コードｘの値を代入することにより元のデ◆

$$f(t)=[\{(g(t)-G-D(x^3+Ex^2+Fx)\}/(x^2+Bx+C)\}-A \quad \cdots\cdots⑤$$

【００３３】以上のようにして復号されたデジタルデータｆ（ｔ）は、データ受け取り側装置２０の図示しない利用回路部へ送られる。

【００３４】次に上述した実施例装置で違法コピーを有効に防止できることを説明する。仮に、上記の処理によ

6

＊【００２２】データ供給側装置１０では、データベース管理部１２がデータ受け取り側装置２０からのデータ要求に基づき、要求のあったソフトウェアのデジタルデータをデータベース１１から取り出して暗号化処理部１３に送る（２Ｓ）。

【００２３】暗号化処理部１３は、前記デジタルデータをデータ受け取り側装置２０から送られてきた識別コードと装置１０内のキーコード発生部１４で発生されたキーコードとを使って暗号化する（３Ｓ）。

【００２４】デジタルデータの暗号化処理の簡略化した例を以下に説明する。いま、暗号化処理されるデジタルデータをｆ（ｔ）、記録媒体ＦＤの識別コードをｘ、キーコードをｙ（ｘ）、暗号化データをｇ（ｔ）で表す。例えば、キーコードｙ（ｘ）を次式①で示される関数に設定する。

※される関数ｈ（ｆ，ｘ，ｙ）とする。

★データｇ（ｔ）は、上記②式にキーコードの関数ｙを代入して、次式③のようになる。

☆体ＦＤに記録された識別コードを、記録媒体ＦＤ自身から読み取り、その識別コードをデータ復号部２５に送る（７Ｕ）。

【００３１】データ復号部２５は、記録媒体ＦＤから読み取られた暗号化データを、データ供給側装置１０から送られてきたキーコードと、識別コード読み取り部２４で読み取られた識別コードとを使って、元のデジタルデータに復号する（８Ｕ）。

【００３２】この復号処理を上記の簡略化された例で説明すれば以下のようになる。データ復号部２５は、暗号化データを復号するための、次式④で表される逆関数ｈ′（ｇ，ｘ，ｙ）をもっている。

◆ジタルデータｆ（ｔ）が復号される。すなわち、元のデジタルデータｆ（ｔ）は次式⑤で再現される。

り所定の記録媒体ＦＤ（以下、第１記録媒体という）に暗号化データが記録され、この第１記録媒体から別の記録媒体（以下、第２記録媒体という）にその暗号化データがコピーされたとする。その第２記録媒体を実施例のデータ受け取り側装置２０にセッティングして復号化し

ようとした場合、識別コード読み取り部２４で読み取られる第２記録媒体の識別コードは第１記録媒体の識別コードとは異なったものになる。したがって、その識別コードをデータ復号部２５に渡しても、第１記録媒体の識別コードを使って暗号化された暗号化データを復号することができないのである。

【００３５】＜第２実施例＞次に、供給されたデジタルデータをユーザ側で適法にコピーするための装置の例を図３を参照して説明する。図３は、適法にコピーをするための構成を追加したデータ受け取り側装置２０の概略構成図である。図中、図１に示した符号と同一の符号で示した構成部分は、上述の第１実施例と同じ構成部分であるので、ここでの説明は省略する。また、データ供給側装置１０も第１実施例と同様であるのでここでの説明は省略する。

【００３６】図３に示したデータ受け取り側装置２０は、供給されたデジタルデータをコピーするための構成として、データ復号部２５で復号されたデジタルデータを新たに暗号化するための暗号化処理部２７、新たな暗号化データを別の記録媒体ＦＤ２に記録するための暗号化データ記録部２８を備えている。

【００３７】最初に記録された記録媒体ＦＤ１から別の記録媒体ＦＤ２にデータをコピーしたい場合、ユーザはデータ受け取り側装置２０の操作部２１を使って、データ供給側装置１０にデータコピーの要求と記録媒体ＦＤ２の識別コードx_2を送る。この要求に基づきデータ供給側装置１０は、新たなキーコードy_2（x_2）をデータ受け取り側装置２０へ送る。このキーコードy_2はデータ受け取り側装置２０の暗号化処理部２７に与えられる。また、ユーザは操作部２１を使って新たな記録媒体ＦＤ２の識別コードx_2を入力する。この識別コードx_2は暗号化処理部２７に与えられる。暗号化処理部２７は、キーコードy_2と識別コードx_2とを使って、データ復号部２５から出力されたデジタルデータを再度、暗号化する。新たな暗号化データg_2は暗号化データ記録部２９によって記録媒体ＦＤ２に記録される。

【００３８】以上のようにしてコピーされた記録媒体ＦＤ２を、元の記録媒体ＦＤ１に変えてデータ受け取り側装置２０にセッティングすれば、データ復号部２５がキーコードy_2と識別コード読み取り部２４で読み取られた記録媒体ＦＤ２の識別コードx_2とを使って記録媒体ＦＤ２の暗号化データg_2を復号することにより、コピーされたデジタルデータｆを利用することができる。

【００３９】＜第３実施例＞図４および図５を参照する。図４はデータ供給側装置の概略構成を示したブロック図、図５はデータ受け取り側装置の概略構成を示したブロック図である。

【００４０】図４に示したデータ供給側装置は、例えばソフトウェア販売店などに設置されるもので、暗号化されたデジタルデータｇを記録媒体ＦＤに記録する暗号化

データ記録部２２を備えている。ユーザが、あるソフトウェアの購入を希望すると、操作部２１Ａからそのソフトウェアが指定される。指定されたソフトウェアのデジタルデータは、操作部２１Ａから入力された記録媒体ＦＤの識別コードｘと、キーコード発生部１４から発生されたキーコードｙとを使って暗号化処理部１３で暗号化される。暗号化されたデジタルデータｇはインターフェース１７を介して暗号化データ記録部２２に与えられ、この暗号化データ記録部２２で記録媒体ＦＤに記録された後にユーザに手渡される（販売される）。暗号化データを解読するためのキーコードｙはプリンタ１６で印字出力されユーザに手渡される。

【００４１】ソフトウェアを購入したユーザは図５に示したデータ受け取り側装置によって暗号化データを復号する。すなわち、データ受け取り側装置では、記録媒体ＦＤの識別コードｘが識別コード読み取り部２４によって読み取られるとともに、操作部２１Ｂを介してユーザによってキーコードｙが入力される。データ復号部２５は、上述した識別コードｘとキーコードｙを使って暗号化データｇを復号し、利用回路部に出力する。

【００４２】

【発明の効果】以上の説明から明らかなように、この発明によれば次の効果を奏する。請求項１に記載のデジタルデータの記録装置によれば、任意のキーコードと記録媒体固有の識別コードとを使って暗号化されたデジタルデータが、その識別コートをもった記録媒体に記録されるので、その記録媒体（第１記録媒体）に記録された暗号化データを別の記録媒体（第２記録媒体）にたとえコピーしても、第２記録媒体の識別コードは第１記録媒体の識別コードとは異なるので、第２記録媒体にコピーされた暗号化データを復号することができない。したがって、この装置によればデジタルデータの違法コピーを有効に防止することができる。

【００４３】また、請求項２に記載の記録媒体によれば、記録媒体にその記録媒体固有の識別コードが書き換え不能に記録されているので、上記の例で第２記録媒体の識別コードを第１記録媒体の識別コードに書き換えることにより暗号化データを復号するということができず、デジタルデータの違法コピーの防止を確実なものにすることができる。

【図面の簡単な説明】

【図１】第１実施例装置の概略構成を示したブロック図である。

【図２】第１実施例装置の動作フローチャートである。

【図３】第２実施例装置のデータ受け取り側装置の概略構成を示したブロック図である。

【図４】第３実施例装置のデータ供給側装置の概略構成を示したブロック図である。

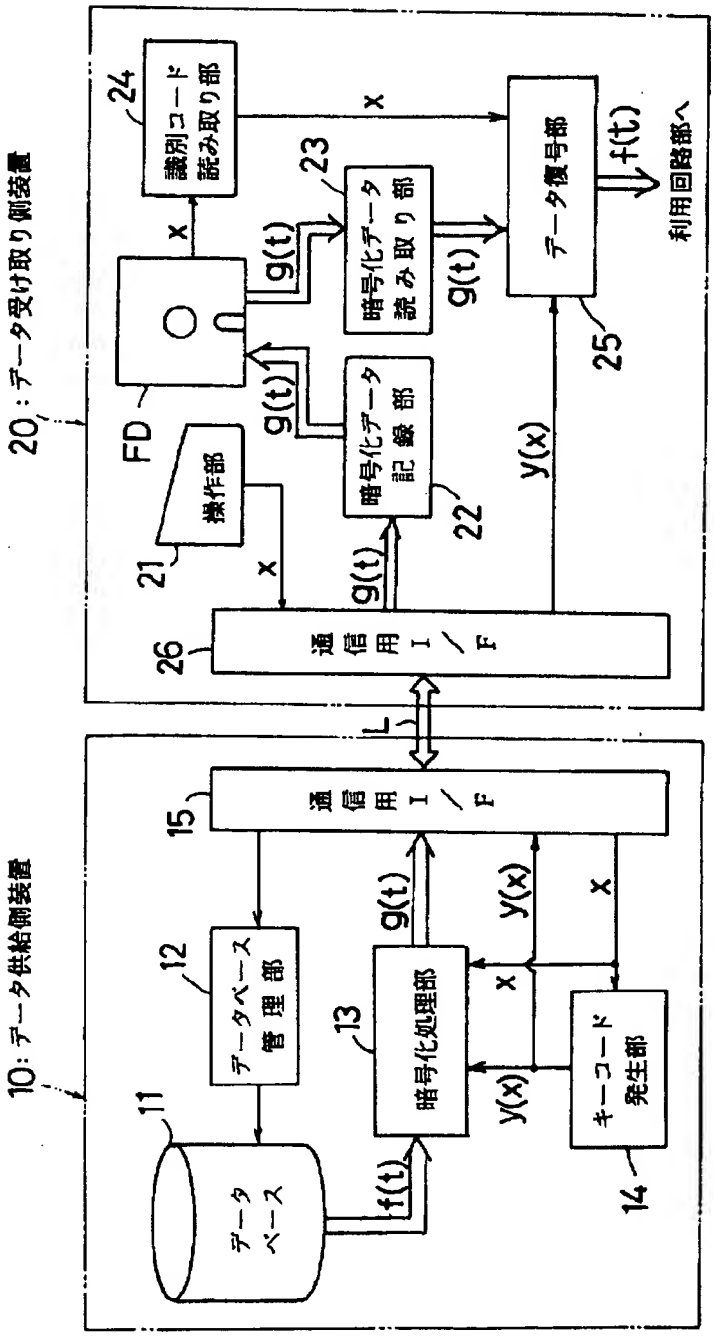
【図５】第３実施例装置のデータ受け取り側装置の概略構成を示したブロック図である。

9　　10

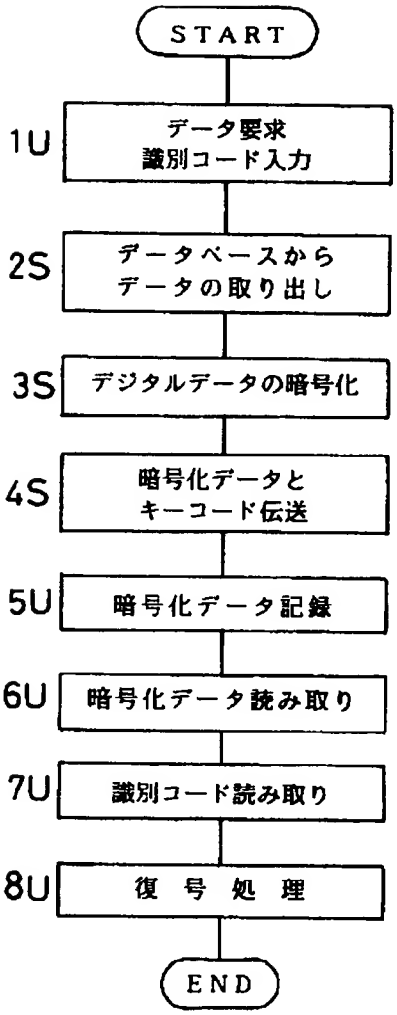
【符号の説明】

１０…データ供給側装置
１１…データベース
１３…暗号化処理部
１４…キーコード発生部
１５，２６…通信用インターフェース
２０…データ受け取り側装置
２１…操作部
２２…暗号化データ記録部
２３…暗号化データ読み取り部
２４…識別コード読み取り部
２５…データ復号部
ＦＤ…記録媒体

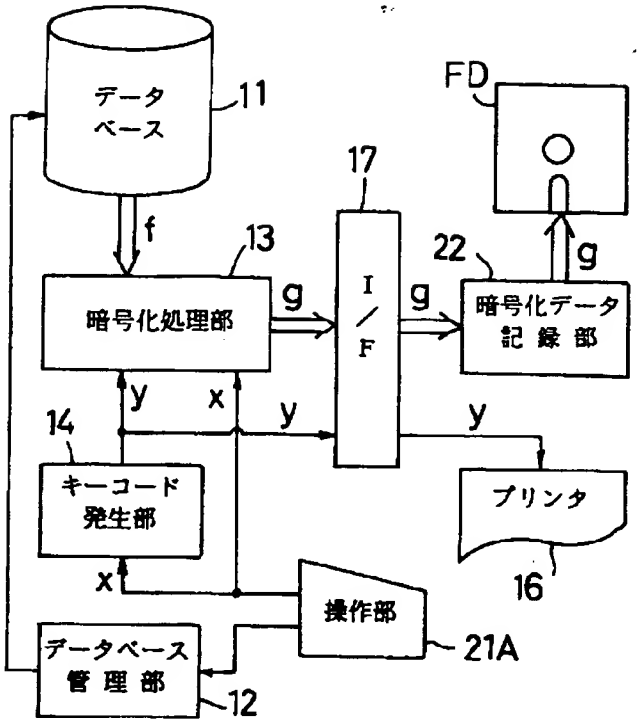
【図１】



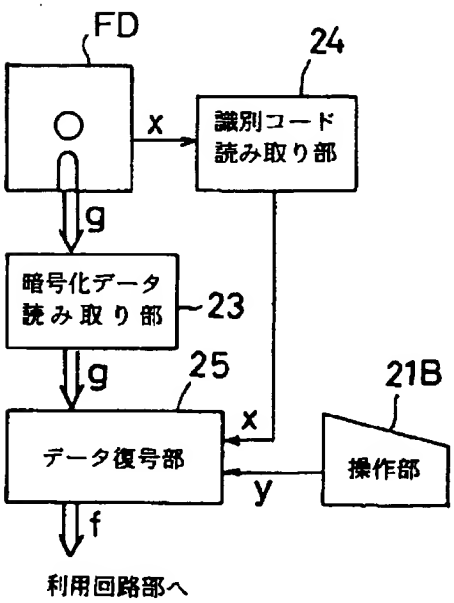
【図2】


START
1U
データ要求
識別コード入力
2S
データベースから
データの取り出し
3S
デジタルデータの暗号化
4S
暗号化データと
キーコード伝送
5U
暗号化データ記録
6U
暗号化データ読み取り
7U
識別コード読み取り
8U
復 号 処 理
END

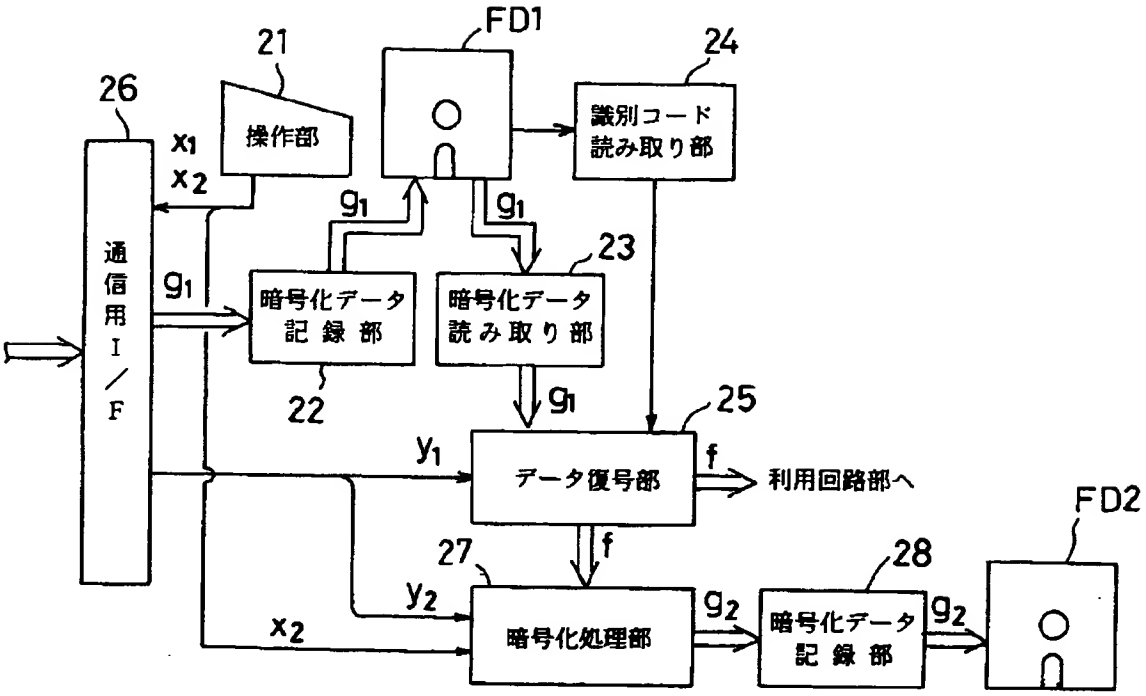
【図4】


データ
ベース
11
FD
17
f
13
22
g
I
/
F
暗号化処理部
g
g
暗号化データ
記 録 部
y
x
y
y
14
キーコード
発生部
プリンタ
x
操作部
21A
データベース
管 理 部
12
16

【図5】


FD
24
x
識別コード
読み取り部
g
暗号化データ
読み取り部
23
g
25
21B
x
データ復号部
操作部
y
f
利用回路部へ

【図３】



フロントページの続き

(51) Int. Cl.⁶	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０６Ｋ　17/00		S		
Ｇ０９Ｃ　1/00		7259－5Ｊ		